'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};		
	said network monitors generating reports of said suspicious activity; and	See '203 claim 1	See '203 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 1	See '203 claim 1
13	The system of claim 12, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
14	The system of claim 12, wherein the integration	See '203 claim 3	See '203 claim 3

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	further comprises invoking countermeasures to a suspected attack.		
15	The system of claim 12, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
16	The system of claim 12, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
17	The system of claim 12, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '203 claim 6	See '203 claim 6
18	The system of claim 12, wherein the plurality of	See '203 claim 7	See '203 claim 7

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	network monitors includes a plurality of service monitors among multiple domains of the enterprise network.		
19	The system of claim 18, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
20	The system of claim 12, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
21	The system of claim 20,	See '203 claim 10	See '203 claim 10

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.		
22	The system of claim 20. wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
1	Method for monitoring an enterprise network, said method comprising the steps of:	See '203 claim 1	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1	See '203 claim 1
	based on analysis of network traffic data,	See '203 claim 1	See '203 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	"One means of detecting anomalous behavior is to monitor statistical measures of user activities on the system. A popular way to monitor statistical measures is to keep *profiles* of legitimate user activities [2,6]. These profiles may include such items as login times, CPU usage, favorite editor and compiler, disk usage, number of printed pages per session, session length, error rate, etc. (T.F. Lunt et al., [7] presents a comprehensive list of possible measures.) The IDS will then use these profiles to compare current user activity with past user activity. Whenever a current user's activity pattern falls outside certain pre-defined thresholds, the behavior is considered anomalous. Legitimate	"The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet*, *mail*, or *finger* is expected to look like)." (171) [SYM_P_0077179] "Certain critical audit records are always passed directly to the expert system (i.e., *notable events*); others are processed locally by the host monitor (i.e., *profiles* and attack *signatures*, which are sequences of noteworthy events which indicate the symptoms

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		behavior that is flagged as intrusive is defined to be a *false alarm*. A major problem with the statistical method is determining exactly what activities and statistical measures provide the highest detection rate and lowest false alarm rate for a particular system. Those statistics that detect an attack on a computer system may differ from system to system depending on the system and its environment; so the measures must be tailored for each particular system. It may also be the case that a particular activity may not be threatening by itself, but when aggregated with other activities, it may constitute an attack. These statistical profiles must be adaptive, i.e., they must be updated regularly, since users may be constantly changing their behavior." (2) [SYM_P_0069281] "The traffic on the network is analyzed by a simple expert system. The types of inputs to the expert system are described below. "The current traffic cast into the ICEM vectors as discussed in the previous subsection is the first type of input. Currently, only the connection vectors and the host vectors are used. The components for these vectors are presented in Tables I and II. "The profiles of expected traffic behavior are the second type input. The profiles consist of expected data paths (viz. which	of attacks) and only summary reports are sent to the expert system." (170) [SYM_P_0077178] "The abnormality of a connection is based on the probability of that particular connection occurring and the behavior of the connection itself." (171) [SYM_P_0077179]

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		systems are expected to establish communication paths to which other systems, and by which service?) and service profiles (viz. what is a typical *telnet, mail, finger,* etc., expected to look like?) Combining profiles and current network traffic gives the NSM the ability to detect anomalous behavior on the network. "The knowledge about capabilities of each of the network services is the third type of input (e.g., *telnet* provides the user with more capability than *ftp* does). "The level of authentication required for each of the services is the fourth type of input (e.g., *finger* requires no authentication, *mail* requests authentication but does not verify it, and *telnet* requires verified authentication). "The level of security for each of the machines is the fifth type of input. This can be based on the NCSC rating of machines, history of past abuses on the different machines, the rating received after running system evaluation software such as SPI or COPS, or simply which machines the security officer has some control over and which machines the security officer has no control over (e.g., a host from outside the local area network). "And the signatures of past attacks is the sixth type of input. Examples include seeing the vertical bar symbol (i.e., |, a Unix	

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		"pipe" symbol) in the receiver address for *mail*, or *finger* connections where the initiating host sends more than 512 bytes to the receiving host. "The data from these sources is used to identify the likelihood that a particular connection represents intrusive behavior, or if a host has been compromised. The security state, or suspicion level, of a particular connection is a function of the abnormality of the connection, the security level of the service being used for the connection, the direction of the connection security level, and the matched signatures of attacks in the data stream for that connection. "The abnormality of a connection is based on the probability of that particular connection occurring and the behavior of the connection itself. If a connection from host A to host B by service C is rare, then the abnormality of that connection is high. Furthermore, if the profile of that connection compared to a typical connection by the same type of service is unusual (e.g., the number of packets or bytes is unusually high for a *mail* connection), the abnormality of that connection is high. "The security level of the service is based on the capabilities of that service and the authentication required by that service. The *tftp* service, for example, has great capabilities with no	

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		authentication, so the security level for *tftp* is high. The *telnet* service, on the other hand, also has great capabilities, but it also requires strong authentication. Therefore, the security level for telnet is *lower* than that of *tftp*. "The direction of connection security level is based on the security levels of the two machines involved and which host initiated the connection. If a low security host connects to, or attempts to connect to a high security host, the direction of connection security level of that connection is high. On the other hand, if a high security host connects to an insecure host, the direction of connection security level is low. "The matched strings consists of the vectors Initiator_X and Receiver_X. Thus it is simply a list of counts for the number of times each string being searched for in the data is matched. "The connection vectors are essentially treated as records in a database, and presentation of the information may be made as simple requests into the database. The default presentation format sorts the connection by suspicion level and presents the sorted list from highest suspicion level to the lowest. Presentations can also be made by specifying time windows for connection, connections from a specific host, connections with a particular string matched, etc.	

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		"The security state, or suspicion level, of a host is simply the maximum security state of its connection vectors over particular window of time. The host vectors are also treated as records into a database, and they may be presented in a similar fashion as the connection vectors." (10-11) [SYM_P_0069289-SYM_P_0069290] "4.5. LAN Monitor "The DIDS LAN monitor is built on the same foundation as UC Davis' Network Security Monitor [5]. Since there is no native LAN audit trail, the LAN monitor is responsible for building its own. The LAN monitor sees every packet on its segment of the LAN. From these packets, the LAN monitor is able to construct higher level objects such as connections (logical circuits), and service requests. In particular, it audits host-to-host connections, services used, and volume of traffic. Like the host based monitor, the LAN monitor uses several levels of analysis to catch the most significant events, for example, sudden changes in network load, the use of security-related services, and network activities such as *rlogin*. As with the host monitor, the LAN monitor retains the audit data for analysis by the director. It also uses and maintains profiles of network behavior, which are updated periodically. Like the host monitor, the LAN monitor provides an agent for	

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		communications with the director. In addition to handling queries of the audit data from the director, this agent gives the director access to a number of network management tools, which are analogous to the host operating system services provided by the host monitor." (13) [SYM_P_0069292]	
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1	See '203 claim 1
2	The method of claim 1, wherein at least one of the network monitors utilizes a signature matching detection method.	"In DIDS, the monitoring and analysis functions are distributed among several components. These components include a *DIDS director*, a collection of *host monitors*, and at least one *LAN monitor*. The host and LAN monitors are primarily responsible for detecting single events and known attack signatures which have a high probability of being relevant to the security of a system; so they must constantly monitor their respective domains." (12) [SYM_P_0069291] "The host monitor incorporates three levels of analysis performed on the HARs. At the lowest level, the host monitor	"The LAN monitor also uses heuristics in an attempt to identify the likelihood that a particular connection represents intrusive behavior. These heuristics consider the capabilities of each of the network services, the level of authentication required for each of the services, the security level for each machine on the network, and signatures of past attacks." (171) [SYM_P_0077179] "In addition to the consideration of external temporal context, the expert system uses time windows to correlate events occurring in temporal proximity. This notion of temporal proximity implements the heuristic that a call to the UNIX *who* command

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		scans each HAR for *notable events*. Notable events are transactions that may be of interest independent of their context (i.e., independent of previous HARs). Examples of notable events include any type of network activity, failed file accesses, accessing system files, and changing a file's access control. At the next higher level, the host monitor looks for *sequences* of events which may be interesting. Known attack signatures or patterns of abuse are examples of sequences which would be of interest." (13) [SYM_P_0069292] "The inference rules provide the ability to recognize a security incident. Each rule takes the general form of a conclusion, which is logically dependent on one or more antecedents. The individual rules are then linked together to form an inference network. That is, the antecedents of a rule are, in general, the conclusions of other rules. The rule base has a hierarchical structure based on a model which describes a security incident in terms of levels of abstraction from the evidence. Reasoning progresses up the hierarchy of abstractions using rules whose conclusions are at a higher level than their antecedents. The current version of the model has seven layers of abstraction. The model provides a framework for developing the rules themselves, as well as for providing the foundation for our argument that the rule base is comprehensive." (14) [SYM_P_0069293]	followed closely by a *login* or *logout* is more likely to be related to an intrusion than either of those events occurring alone. Spatial context implies the relative importance of the source of events. That is, events related to a particular user, or events from a particular host, may be more likely to represent an intrusion than similar events from a different source. For instance, a user moving from a low-security machine to a high-security machine may be of greater concern than a user moving in the opposite direction. The model also allows for the correlation of multiple events from the same user or source. In both of these cases, the multiple events are more noteworthy when they have a common element than when they do not." (172) [SYM_P_0077180] "We are designing a signature analysis component for the host monitor to detect events and sequences of events that are known to be indicative of an attack, based on a specific context." (174) [SYM_P_0077182]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

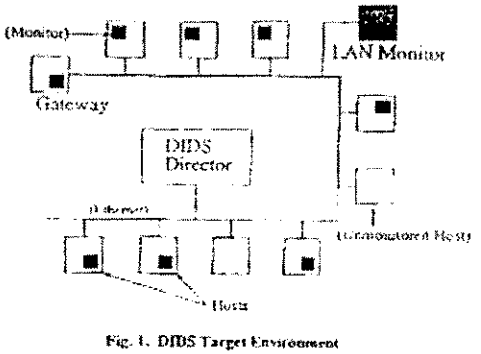
'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		"And the signatures of past attacks is the sixth type of input. Examples include seeing the vertical bar symbol (i.e., |, a Unix "pipe" symbol) in the receiver address for *mail*, or *finger* connections where the initiating host sends more than 512 bytes to the receiving host." (11) [SYM_P_0069290]	
3	The method of claim 2, wherein the monitor utilizing a signature matching detection method also utilizes a statistical detection method.	"4.5. LAN Monitor "The DIDS LAN monitor is built on the same foundation as UC Davis' Network Security Monitor [5]. Since there is no native LAN audit trail, the LAN monitor is responsible for building its own. The LAN monitor sees every packet on its segment of the LAN. From these packets, the LAN monitor is able to construct higher level objects such as connections (logical circuits), and service requests. In particular, it audits host-to-host connections, services used, and volume of traffic. Like the host based monitor, the LAN monitor uses several levels of analysis to catch the most significant events, for example, sudden changes in network load, the use of security-related services, and network activities such as *rlogin*. As with the host monitor, the LAN monitor retains the audit data for analysis by the director. It also uses and maintains profiles of network behavior, which are updated periodically. Like the host monitor, the LAN monitor provides an agent for communications with the director. In addition to handling queries of the audit data from the director, this agent gives the	"Like the host monitor, the LAN monitor consists of a *LAN event generator* (LEG) and a *LAN agent*. The LEG is currently a subset of UC Davis' NSM [3]. Its main responsibility is to observe all of the traffic on its segment of the LAN to monitor host-to-host connections, services used, and volume of traffic. The LAN monitor reports on such network activity as *rlogin* and *telnet* connections, the use of security-related services, and changes in network traffic patterns." (169) [SYM_P_0077177] "An event reported by a LAN monitor is called a network audit record (nar). The record syntax is: nar(Monitor-ID, Source_Host, Dest_Host, Time, Service, Domain, Status)." (172) [SYM_P_0077180] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		director access to a number of network management tools, which are analogous to the host operating system services provided by the host monitor." (13) [SYM_P_0069292] "In DIDS, the monitoring and analysis functions are distributed among several components. These components include a *DIDS director*, a collection of *host monitors*, and at least one *LAN monitor*. The host and LAN monitors are primarily responsible for detecting single events and known attack signatures which have a high probability of being relevant to the security of a system; so they must constantly monitor their respective domains." (12) [SYM_P_0069291] "And the signatures of past attacks is the sixth type of input. Examples include seeing the vertical bar symbol (i.e., |, a Unix "pipe" symbol) in the receiver address for *mail*, or *finger* connections where the initiating host sends more than 512 bytes to the receiving host." (11) [SYM_P_0069290]	circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179] "The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet*, *mail*, or *finger* is expected to look like)." (171) [SYM_P_0077179] "The host monitor (Fig. 3) examines each audit record to determine if it should be forwarded to the expert system for further evaluation. Certain critical audit records are always passed directly to the expert system (i.e., *notable events*); others are processed locally by the host monitor (i.e., *profiles* and attack *signatures*, which are sequences of noteworthy events which indicate the symptoms of attacks) and only summary reports are sent to the expert system." (170) [SYM_P_0077178]
4	The method of claim 1, wherein integrating comprises correlating intrusion reports	See '203 claim 2	See '203 claim 2

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	reflecting underlying commonalities.		
5	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
6	The method of claim 1, wherein the plurality of network monitors includes an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
7	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
8	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN managers, like our previous work, a network security monitor (NSM), as well." (1) [SYM_P_0069280] **103:**	"In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		NetRanger: NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-82], 1-6 [SYM_P_0074979], 2-3 to 2-4 [SYM_P_0074996-97]	 Fig. 1. DIDS Target Environment [SYM_P_0077184]
9	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8	See '203 claim 8
10	The method of claim 9,	See '203 claim 8	See '203 claim 8

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.		
11	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
12	The method of claim 11, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
13	The method of claim 11,	See '203 claim 11	See '203 claim 11

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	wherein the plurality of the domain monitors within the enterprise network establish peer-to-peer relationships with one another.		
14	An enterprise network monitoring system comprising:	See '212 claim 1	See '212 claim 1
	a plurality of network monitors deployed within an enterprise network;	See '212 claim 1	See '212 claim 1
	said plurality of network monitors detecting suspicious network activity	See '212 claim 1	See '212 claim 1
	based on analysis of network traffic data,	See '212 claim 1	See '212 claim 1
	wherein at least one of the network monitors utilizes a statistical detection method;	See '212 claim 1	See '212 claim 1
	said network monitors generating reports of said suspicious activity; and	See '212 claim 1	See '212 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical	See '212 claim 1	See '212 claim 1

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	monitors adapted to automatically receive and integrate the reports of suspicious activity.		
15	The system of claim 14, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
16	The system of claim 14, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
17	The system of claim 14, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
18	The system of claim 14, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
19	The system of claim 14, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8	See '212 claim 8
20	The system of claim 14, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8	See '203 claim 8
21	The system of claim 20, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
22	The system of claim 14, wherein the plurality of network monitors include a	See '203 claim 9	See '203 claim 9

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'212 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.		
23	The system of claim 22, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10
24	The system of claim 22, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '203 claim 1	See '203 claim 1
	deploying a plurality of network monitors in the enterprise network;	See '203 claim 1	See '203 claim 1
	detecting, by the network monitors, suspicious network activity	See '203 claim 1	See '203 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};	See '203 claim 1	See '203 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '203 claim 1	See '203 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '203 claim 1	See '203 claim 1
2	The method of claim 1, wherein integrating	See '203 claim 2	See '203 claim 2

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	comprises correlating intrusion reports reflecting underlying commonalities.		
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8	See '212 claim 8
7	The method of claim 1, wherein at least one of said network monitors utilizes a statistical detection method.	See '212 claim 1	See '212 claim 1
8	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8	See '203 claim 8
9	The method of claim 8, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service	See '203 claim 8	See '203 claim 8

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	monitors within the domain monitor's associated network domain.		
10	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
11	The method of claim 10, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
12	The method of claim 10, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
13	An enterprise network monitoring system comprising:	See '615 claim 1	See '615 claim 1
	a plurality of network monitors deployed within an enterprise network,	See '615 claim 1	See '615 claim 1
	said plurality of network monitors detecting suspicious network activity	See '615 claim 1	See '615 claim 1
	based on analysis of network traffic data selected from one or more of the following categories: {network packet data transfer	See '615 claim 1	See '615 claim 1

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet, network connection acknowledgements, and network packets indicative of well-known network-service protocols};		
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1	See '615 claim 1
14	The system of claim 13, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
15	The system of claim 13, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
16	The system of claim 13, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4

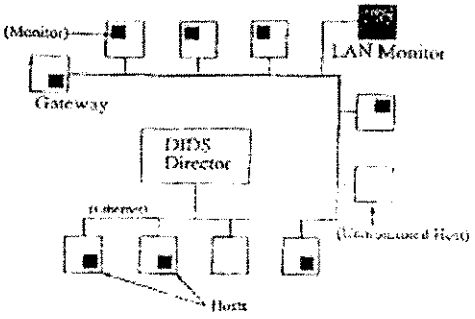
Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
17	The system of claim 13, wherein the enterprise network is a TCP/IP network.	See '203 claim 5	See '203 claim 5
18	The system of claim 13, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	See '212 claim 8	See '212 claim 8
19	The system of claim 13, wherein the plurality of network monitors includes a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 8	See '203 claim 8
20	The system of claim 19, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
21	The system of claim 13, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
22	The system of claim 21, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to	See '203 claim 10	See '203 claim 10

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	automatically receive and integrate the reports of suspicious activity.		
23	The system of claim 21, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
34	A computer-automated method of hierarchical even monitoring and analysis within an enterprise network comprising:	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a gateway;	"The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN managers, like our previous work, a network security monitor (NSM), as well." (1) [SYM_P_0069280]	"In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			 Fig. 1. DIDS Target Environment [SYM_P_0077184]
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
35	The method of claim 34, wherein said	See '203 claim 2	See '203 claim 2

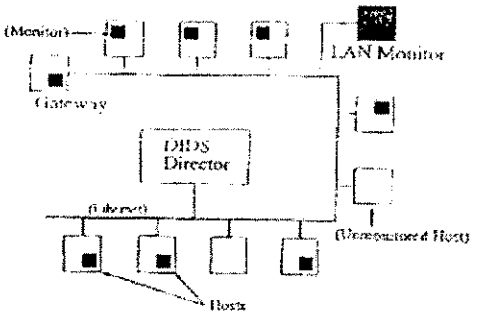
Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	integrating comprises correlating intrusion reports reflecting underlying commonalities.		
36	The method of claim 34, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
37	The method of claim 34, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
38	The method of claim 34, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1	See '615 claim 1
39	The method of claim 34, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
40	The method of claim 39, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of	See '203 claim 8	See '203 claim 8

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	service monitors within the domain monitor's associated network domain.		
41	The method of claim 34, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
42	The method of claim 41, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10
43	The method of claim 41, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
44	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a router;	"The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN managers, like our previous work, a network	"In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		security monitor (NSM), as well." (1) [SYM_P_0069280] **103:** NetRanger: NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-82], 1-6 [SYM_P_0074979], 2-3 to 2-4 [SYM_P_0074996-97]	development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]  Fig. 1. DIDS Target Environment [SYM_P_0077184] **103:** NetRanger: NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-82], 1-6 [SYM_P_0074979], 2-3 to 2-4 [SYM_P_0074996-97]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	detecting, by the network monitors, suspicious network activity based on analysis of the network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
45	The method of claim 44, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
46	The method of claim 44, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
47	The method of claim 44, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
48	The method of claim 44, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet	See '615 claim 1	See '615 claim 1

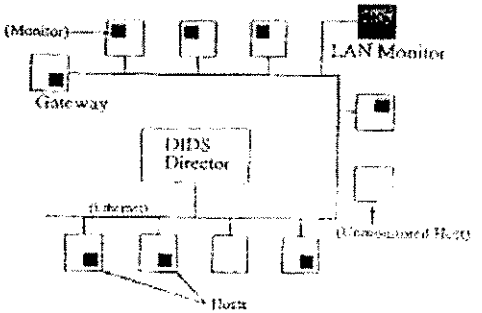
Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	data volume, network connection requests, network connection denials, error codes included in a network packet}.		
49	The method of claim 44, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	See '203 claim 7	See '203 claim 7
50	The method of claim 49, wherein said receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
51	The method of claim 44, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
52	The method of claim 51, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 10	See '203 claim 10

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
53	The method of claim 51, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
64	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	See '615 claim 1	See '615 claim 1
	deploying a plurality of network monitors in the enterprise network, wherein at least one of the network monitors is deployed at a firewall;	**103:** "The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN managers, like our previous work, a network security monitor (NSM), as well." (1) [SYM_P_0069280] SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856].	**103:** "In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			 Fig. 1. DIDS Target Environment [SYM_P_0077184] SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856].
	detecting, by the network monitors, suspicious network activity based on analysis of network traffic data;	See '615 claim 1	See '615 claim 1
	generating, by the monitors, reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1

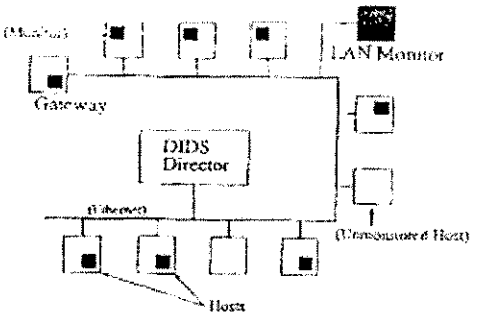
Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	See '615 claim 1	See '615 claim 1
65	The method of claim 64, wherein said integrating comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
66	The method of claim 64, wherein said integrating further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
67	The method of claim 64, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
68	The method of claim 64, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1	See '615 claim 1
69	The method of claim 64, wherein said deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise	See '203 claim 7	See '203 claim 7

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	network.		
70	The method of claim 69, wherein said receiving and integrating is preformed by a domain monitor with respect to a plurality of service monitors within the domain monitor's associated network domain.	See '203 claim 8	See '203 claim 8
71	The method of claim 64, wherein said deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
72	The method of claim 71, wherein said receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See'203 claim 10	See'203 claim 10
73	The method of claim 71, wherein the plurality of domain monitors within the enterprise network establish peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11
84	An enterprise network monitoring system comprising:	See '615 claim 1	See '615 claim 1
	a plurality of network monitors deployed	"The generalized distributed environment is	"In addition to the current host monitor, which is designed to

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	within an enterprise network, wherein at least one of the network monitors is deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers, firewalls}, said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data:	heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN managers, like our previous work, a network security monitor (NSM), as well." (1) [SYM_P_0069280] **103:** NetRanger: NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-82], 1-6 [SYM_P_0074979], 2-3 to 2-4 [SYM_P_0074996-97] SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856].	detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]  Fig. 1. DIDS Target Environment [SYM_P_0077184]
	said network monitors generating reports of said suspicious activity; and	See '615 claim 1	See '615 claim 1

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	one or more hierarchical monitors in the enterprise network, the hierarchical monitors adapted to automatically receive and integrate the reports of suspicious activity.	See '615 claim 1	See '615 claim 1
85	The system of claim 84, wherein the integration comprises correlating intrusion reports reflecting underlying commonalities.	See '203 claim 2	See '203 claim 2
86	The system of claim 84, wherein the integration further comprises invoking countermeasures to a suspected attack.	See '203 claim 3	See '203 claim 3
87	The system of claim 84, wherein the plurality of network monitors include an application programming interface (API) for encapsulation of monitor functions and integration of third-party tools.	See '203 claim 4	See '203 claim 4
88	The system of claim 84, wherein said network traffic data is selected from one or more of the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet}.	See '615 claim 1	See '615 claim 1
89	The system of claim 84, wherein the plurality of network monitors includes a	See '203 claim 7	See '203 claim 7

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'615 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	plurality of service monitors among multiple domains of the enterprise network.		
90	The system of claim 89, wherein a domain monitor associated with the plurality of service monitors within the domain monitor's associated network domain is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 8	See '203 claim 8
91	The system of claim 84, wherein the plurality of network monitors include a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of the enterprise network.	See '203 claim 9	See '203 claim 9
92	The system of claim 91, wherein an enterprise monitor associated with a plurality of domain monitors is adapted to automatically receive and integrate the reports of suspicious activity.	See '203 claim 10	See '203 claim 10
93	The system of claim 91, wherein the plurality of domain monitors within the enterprise network interface as a plurality of peer-to-peer relationships with one another.	See '203 claim 11	See '203 claim 11